

# INTERNATIONAL PRIVACY COMPLIANCE: WHAT YOU NEED TO KNOW

PANEL 3: SELECT ISSUES  
OFFSHORING RISKS  
November 4, 2004

Maureen A. Young  
Bingham McCutchen LLP

(415) 393-2788

[maureen.young@Bingham.com](mailto:maureen.young@Bingham.com)

© 2004 Maureen Young - All rights reserved

**BINGHAM McCUTCHEN**

## I. Major Increase in Offshored Work

- **Increased Volume and More Functions.** As you know, the volume and the types of work being “offshored” by U.S. companies has dramatically increased in the last few years. At one point, the offshored work consisted primarily of IT work, such as computer programming and software development and maintenance. Today, U.S. companies are looking to offshore all types of business processing functions, as well as customer support and call centers, human resources, accounting, tax services, paralegal work, and a litany of other corporate functions.
- **Motivation.** The motivation for offshoring is primarily to derive cost savings from less expensive labor markets and the

attractive tax benefits offered by foreign countries, and to a lesser extent, to tap into a broader field of trained professionals.

- **Countries.** The countries to which work is being offshored is broad, but includes India, Pakistan, Russia, China, the Czech Republic, and the Philippines. Many of these countries still have less developed privacy laws, intellectual property regimes and criminal and civil law enforcement systems.
- **Forms of Offshoring.** The offshoring is occurring in many forms. It is occurring directly, through outsourcing arrangements with foreign companies or through agreements with U.S. companies who have foreign operations or subsidiaries, or through the company itself deciding to establish its own foreign operation or foreign subsidiary. But offshoring is also occurring indirectly through existing outsourcing arrangements in which service providers, if not

subject to contractual restrictions, are offshoring work to foreign subcontractors or deploying foreign-based operations.

- **Backlash in the U.S.** The result of increased offshoring has been political backlash regarding the loss of U.S. jobs and fears regarding the protection of confidential customer data. The incident regarding the medical transcriber in Pakistan who threatened to release confidential patient records if she wasn't paid is now infamous.
- **Increased regulatory and legislative scrutiny.** Another by-product of increased offshoring is increased regulatory and legislative scrutiny of how well the offshoring arrangements deal with privacy, confidentiality of customer information and information security. The increased scrutiny means that companies need to do more due diligence before entering into

offshoring arrangements, obtain tougher contractual protections and monitoring the offshored operation more closely.

## **II. Uncertain Legislative Environment**

- On the legislative front, many state and federal bills which would restrict offshoring arrangements were proposed this year.
- On the state level, 5 bills involving offshoring were passed by the Assembly and Senate and sent to Governor Schwarzenegger this year, but he vetoed them. Next year may go differently. The vetoed bills were:
  - AB 1829 (Liu) (provided that any contract for a state agency or local government be performed solely with

workers in the U.S. and further provided that any no state funds be expended for training employees located in foreign countries)

- AB 2715 (Reyes) (provided that an entity conducting business in California have their customer service employees disclose the location upon the request of a California resident)
- AB 3021 (Committee on Labor and Employment) (provided that an employer with more than 250 employees include in its wage report the number of employees inside of California, in other states, and outside the U.S.)
- SB 888 (Dunn) (prohibited the performance of any work involving information that is essential to homeland security at a worksite outside the U.S.)

- SB 1492 (Dunn) (prohibited a health care business from transmitting individually identifiable health information to a site outside the U.S. unless specified notice and authorization requirements were satisfied).
- On the federal front, a multitude of bills were introduced, in addition to offshoring becoming an issue in the presidential campaign. The bills did not approach being enacted, but versions of same are likely to be introduced again next year. A sampling of the proposed legislation includes the following:
  - S. 2481 (Nelson) (The “Increasing Notice of Foreign Outsourcing Act,” a bill to require that notices to consumer of health and financial services include information on the outsourcing of sensitive personal information abroad, to require the appropriate federal agencies to prescribe

regulations to ensure the privacy and security of sensitive personal information outsourced abroad, and to establish requirements for foreign call centers)

- H.R 4366 (Markey) (“Personal Data Offshoring Protection Act of 2004, a bill to prohibit the transfer of personal information to any person outside the U.S., without notice and consent).
- Other federal proposals included establishment of a U.S. regulatory certification of foreign outsourcing companies, such as an FTC certification, and expansion of coverage under the Worker Adjustment and Retraining Notification Act (known as the “WARN” Act) which would require that a business submit to the federal government advance notice of any offshoring arrangement that will result in a certain number of U.S. jobs being eliminated.

- **Expect restrictions on offshoring arrangements.** Although legislation may not have been enacted this year, we should expect that legislative and regulatory restrictions on offshoring will eventually be imposed. The likely impact of such restrictions will be to “up the ante” by increasing the compliance and operational costs associated with offshoring. In drafting offshoring contracts, you should anticipate:
  - An ability to terminate the offshoring arrangement in the event that legal restrictions bar certain information from being offshored and an ability to change cost structures in the event the legislation imposes tax disadvantages or other costs that make the offshoring arrangement economically unattractive

- Contractual provisions which would allow you to provide notice and disclosure to customers about the offshoring arrangements, and possibly, to accommodate a customer's right to "opt out" of the offshoring arrangement

### **III. Key Risks Presented By Offshoring Arrangements**

- **Other Key Risks.** In addition to legislative and regulatory restrictions which may be imposed on offshoring arrangements, there are a number of other key risks which need to be analyzed before entering into an offshoring arrangement:
  - Country risk
  - Compliance risk
  - Contractual risk
  - Reputational risk

- To address these risks, one should deploy:
  - Greater vetting and evaluation of the risks, including enhanced internal review and additional corporate authorizations
  - Enhanced due diligence regarding the offshore service provider and their operations
  - Additional responsibility for monitoring and compliance functions
  - More stringent contractual requirements
- **Country risk.**
  - Requires due diligence and ongoing monitoring of evaluation of the legal, economic, social and cultural and political circumstances in the foreign country

- What political risks could result in instability in the performance of the contract or its enforceability?
- Analysis of the applicable laws in the foreign jurisdiction.
- Assessment of the local law enforcement environment - to what extent can contractual violations, criminal liabilities and torts be successfully pursued in the local courts?
- What employee-related risks are associated with doing business in the foreign jurisdiction, *e.g.*, the ability to effectively conduct background checks or enforce claims against the wrongful acts of employees? What additional costs and/or restrictions may local labor laws impose on the arrangement?
- What contingency plans and exit strategies are available to your company if it needs to move its work elsewhere?

- What are the chances that your company's assets may be confiscated by the foreign jurisdiction? Similarly, what is the likelihood of the foreign government imposing confiscatory tax assessments?
- **Compliance Risk.** An assessment of compliance risk should include:
  - A review to ensure that nothing in the offshoring arrangement will impede the company's ability to comply with all applicable U.S. or other laws or the ability of your company's regulators to supervise operations in: (i) the U.S. and (ii) the foreign jurisdiction.
  - An evaluation of how the foreign country's data protection scheme meshes with U.S. privacy and data security

requirements and other foreign privacy laws impacting your customer base.

- A due diligence and assessment process which evaluates the operations and financial circumstances of the vendor, local law, local business practices and accounting standards in the foreign country, and the relative strengths and weaknesses of the law enforcement and judicial system in the foreign country.

- **Contractual Risk.** An assessment of contractual risk should include:

- A careful selection of the choice of law and venue for dispute resolution.
- Development of effective processes for monitoring and oversight.

- Specific provisions permitting your company and its regulators to have access to information, including the vendor's express agreement to permit your regulators to conduct examinations of its operations on site and through document requests.
- Rights for your company to conduct regular and periodic audits, with requirements that your company be regularly and promptly provided with reports of independent financial and operation audits.
- **Reputation Risk.** An assessment of the reputation risks should include:
  - An evaluation of the specific circumstances and the likely scenarios which may result in damage to your company

through poor service, disruption of service, violations of consumer law, etc.

- Specific attention to potential confidentiality and privacy breaches and intellectual property piracy.
- Focus on well-developed information security and business continuity plan and procedures, with ongoing monitoring and testing.

#### **IV. Additional Due Diligence Required**

- **Enhanced Due Diligence.** In addition to the usual due diligence and analysis conducted with respect to vendors, offshoring arrangements present some additional issues that merit evaluation:

- Financial, managerial, organizational, operational and customer service due diligence:
- Thorough assessment of the business case justifying going offshore for the services. Are mission critical or “core” corporate functions being outsourced and if so, is this necessary? Development and review of internal policies re: what types of services should be offshored and what types should generally be conducted domestically. Where does the arrangement fall in terms of the risks related to outsourcing of IT functions v. business processing functions in which customer information may need to be shared?
- Are the savings anticipated conservatively projected; is there leeway for unanticipated costs resulting from the need for further training, re-doing work, or revising service

standards? (It is estimated that offshoring arrangements often take 3 years or more from their commencement dates before savings are realized.)

- With respect to evaluating the full costs of moving to an offshoring arrangement, have the vendor's operational and customer service abilities been adequately assessed? Will the vendor be able to provide adequate training to its employees? What things may be likely to go wrong? How will customers react to the use of an offshore service company?
- Is your company's knowledge of the financial and managerial strength of the vendor adequate, or does a consultant with more country risk knowledge need to be brought in?

- Review of recent independent audits; obtain a commitment that your company will have an ongoing ability to audit the vendor.
- Does the vendor hold key international security and audit certifications (*e.g.*, ISO 17799 or BS 7799)? Can full SAS 70 audits be performed with confidence?
- On-site evaluation and the ability of your company's personnel to effectively manage from afar. How many dedicated vendor personnel are required for management, oversight and compliance functions? Is it necessary or valuable to also have dedicated management of your company on the ground in the offshore jurisdiction?
- Does your company really know who it is doing business with and who the vendor is doing business with? Is there adequate knowledge of the vendor's affiliates, interests and

principal relationships with entities and persons in other countries?

- Be sure that the outsourcer is not outsourcing your company's work to other entities or parties, particularly, to ones in another country. (For example, the leading Indian service providers have been moving operations to China and other places with even lower labor costs than those in India.)

- **Legal, Regulatory, and Compliance Due Diligence.**

- Legal Structure. Careful attention needs to be paid to what legal structure is deployed for the delivery of the services. In many instances, a third party vendor will be chosen. Other options may include providing the services through a subsidiary of your company, or using employees of your

company in its foreign offices. Consideration of alternative structures requires additional regulatory assessment and due diligence.

- What specific regulations will apply to the offshoring arrangement and will the vendor be able to successfully comply with all applicable U.S. and foreign laws?
- Specifically, how well will the vendor be able to meet U.S. privacy and security requirements, as well as those of the European Union or other applicable foreign data protection regimes?
- Required Licenses. Depending on the nature of the business being offshored and the legal structure deployed for the offshoring arrangements, diligence needs to be conducted prior to entering into the arrangement re: what U.S. or foreign business licenses may be necessary for the

vendor to perform the services on behalf of your company, what the process, costs, and processing timeframes may be in obtaining those licenses, and what compliance issues may arise with respect to holding such licenses.

- **Human Resources Issues.**

- Requires good knowledge of local labor laws and business practices.
- Examination of the quality, depth and reliability of employee background clearances and the vendor's ongoing knowledge and monitoring of employees. U.S. companies often conduct background checks of employees which include review of work history and references, credit bureau information, criminal records and often, drug

testing. The ability to obtain the same types of reviews in many other countries is questionable.

- Local business/legal culture - is there an higher incident of intellectual property piracy and identity theft issues, coupled with a weak law enforcement system?
- How will the vendor cultivate strong middle management, which is often lacking in companies in the prevailing offshoring jurisdictions?
- Is there high employee turnover at the vendor, creating service instability and security risks, and how will retention issues be addressed?
- Will cultural differences result in staff and management requiring additional training or work needing to be redone, thereby, incurring additional costs? For example, it is often observed that in India, the style of English writing is more

formal, resulting in U.S. companies rewriting work product. Any consequences if English is a second language for the employees? Any communication difficulties resulting from the employees not thinking in English? In the customer service areas, will there be a need for accent “Americanization” training?

- What other local cultural issues must be taken into account - *e.g.*, different holidays, patterns of discrimination, interpersonal behavior?
- How will your company address any morale issues for domestic staff who may or will be downsized? What severance terms will be provided? Will there be re-training benefits?
- How will your company deal with any customer or community concerns about the offshoring arrangement?

Press releases, standby statements, need for incident response plans.

## **V. Special Emphasis on Protection of Confidential Information, Information Security and Business Continuity.**

Offshoring contracts need heightened emphasis on:

- **Confidentiality and information security requirements:**
  - Well-developed confidentiality provisions in the contract with express “needs to know” terms.
  - Each of the vendors’ employees working on the services should sign a confidentiality agreement.
  - There should be an express prohibition against sharing any of your company’s confidential information with the

vendor's affiliates or third parties without your company's prior written consent.

- Confidential information must be used “for the purpose” only. There should be an express prohibition against the vendor using the information for marketing of other services by it or other parties.
- Consideration of enforceability issues - if an employee left the vendor with your company's confidential information, would the vendor or your company be able to successfully enforce your company's rights?
- Return of documents upon termination - how would your company attain confidence that all of its confidential information had been returned? Requires additional contractual protections for verification, etc.

- If the offshored services affect European customers, how will your company address their heightened concern for data protection and privacy and compliance with applicable elements of the European Union directives? Similar issues for customers in other countries with strict privacy law regimes.
- Preparation by the vendor of a tailored information security plan is key. In addition to committing to comply with your company's information security policies, the vendor should commit in the contract to develop an information security plan designed to protect your company's confidential information. The plan should be reviewed and approved your company and be updated regularly.
- The security plan should cover elements specified by your company. In addition, it should include monitoring and

testing procedures, along with the right of your company to conduct its own audit and intrusion testing.

- The security plan should be drafted and reviewed prior to the parties entering into the offshoring agreement when your company has the most leverage as to its scope and content.
- The plan should include the requirement that the vendor contact your company's security incident command central in the event of a known or suspected security intrusion. The plan should include a written response program in the event that there is an information security breach.
- The plan should include provisions for returning your company's confidential information, with verification to you, or disposing of the information in a manner which meets your requirements and recent regulatory guidance.

- Where customer information is being shared, it may be necessary to include some specific security measures, such as, restriction of access to the information to only designated employees; restrictions to access specific physical areas where the customer information is being used or stored; installation of software to encrypt key portions of the customer information, which then cannot be viewed by the employees; restrictions on the employees' ability to print out or e-mail certain database information; and restrictions on employees' access to the Internet from their work stations, etc.
- Business continuity plans:
  - Must go beyond the traditional disaster recovery plan in scope, to include lack of service as a result of terrorism,

strikes, lack of supplies, political unrest and other adverse circumstances which may be projected -- the plan must have carefully assessed the possible contingencies.

- The plan should tie in with the force majeure clause - the vendor should not be able to rely on the force majeure clause to be excused from performance for events beyond its control unless it has already “deployed the applicable elements” of the business continuity plan.
- The plan should set forth alternative service arrangements, which should include workarounds by itself, as well as alternatives with third party service providers. The services available through third party service providers should be detailed with contact information and anticipated terms.
- The business continuity plan must be reviewed and approved by your company and be updated regularly.

- The plan should cover elements specified by your company. In addition, it should include testing procedures, along with the right of your company to conduct its own business continuity testing of the vendor's services. Conversely, the vendor should commit to assist and cooperate in the testing of your company's own business continuity plan.
- The business continuity plan should be drafted and reviewed prior to the parties entering into the agreement when your company has the most leverage as to its scope and content.
- The plan must ensure timely access to critical information and service resumption.

- Your company needs to thoroughly understand the vendor's infrastructure limitations and have planned for them.
- Attention must be paid to specific national or geographic restrictions.
- The plan must build in redundancy, especially redundancy at significant distances. For example, the vendor should not have all its disaster recovery sites in its own country, especially for mission critical services -- they should be spread globally.
- The contract should contain an express contractual commitment by the vendor to provide transition/termination services (irrespective of whether the termination by your company was for cause or for

convenience) for a period of at least 180 days and to cooperate/assist with the transition as needed.

## **VI. Additional Contractual Protections -- “Vendor Management Writ Large.”**

In addition to addressing the foregoing concerns and in addition to the normal protections pursued for effective vendor management, your company should also negotiate for some specific protective terms in the offshoring contract, such as the following:

- Careful choice of law and forum in the contract -- important issues. Ideally, the contract should usually specify a U.S. state’s law as the governing law, with a domestic forum, but interlocutory relief in the foreign country should also be

available to your company. Your attorneys should be consulted on any proposed governing law/forum variations.

- Strict control over use of affiliates and any subcontractors - express prohibition against the use of affiliates or subcontractors without your company's prior written consent.
- Express provisions regarding the oversight and monitoring process, including, if applicable, a customers' complaint reporting and resolution process.
- Express provisions regarding the type, scope and frequency of reports expected from vendor and service levels associated with the failure to meet the reporting requirements on a timely basis.
- "Captured Vendor." In addition to the strict confidentiality, privacy, security and business continuity requirements discussed above, your company may consider whether from a

conflict of interest, confidentiality, privacy and security viewpoint, it needs the vendor to agree to exclusively provide the specific services to your company and to no other company. (There are some drawbacks to this that need to be weighed.)

- No exclusivity commitment on part of your company. Your company should not commit to exclusively retain only the vendor for the services - you need the flexibility to move to other alternatives if issues with the vendor's performance or other concerns arise.
- Your company should have the ability to review the vendor's employee hiring and background clearance process.
- Your company should have the right to request that any employee of the vendor working on the services be removed for performance reasons. (Provisions like these need to be

crafted carefully because in certain foreign jurisdictions, actions that may be construed to be exercises of control by your company over the vendor's employees may cause those vendor employees to be deemed to be employees of your company.)

- The vendor should be prohibited from retaining any employee who has committed the equivalent of a felony or fraud offense; the vendor should provide representations and warranties that it will not retain employees with such criminal records and indemnify your company from any losses resulting from employees who engage in such crimes.
- Provisions which allow your company to engage in strong financial monitoring of the vendor.
- Strong rights of your company to audit the vendor's operations itself and to require third party audits of the vendor.

- Flexibility should be built into the contractual terms - ability to change the contract to take into account necessary changes in service standards and costs based on compliance and relationship issues -- include provisions which allow your company to alter its service requests without payment of “change order” penalties.
- Scope of service should be clearly defined in the contract and its exhibits, but include a catch-all that the vendor shall also perform such additional services as are “inherent in the scope” of the express services.
- Well-developed service performance standards with milestones and credits back to your company for failure of the vendor to meet specific service levels; express provisions setting timeframes and other parameters for corrections or

workarounds. Clear standards for when failure to meet certain service levels constitutes material breach.

- Need for benchmarking; performance review -- requirements that the vendor change its practices if the practices if do not meet your company's requirements, industry standards or compliance standards. Provisions for permitting the service levels to be changed over time as knowledge of the vendor's performance shortcomings or other issues in the working relationship with the vendor become known.
- Many, strong termination rights for your company -- express terms for what actions or omissions by the vendor constitute material breach.
- Special attention to the length of the term and the renewal provisions of the agreement - your company needs in the face

of uncertainty to not get locked in, while at the same time, being able to maintain stability in service.

- Only your company, and not the vendor, should have the right to terminate for convenience.
- “Evolution of services” provisions -- does the contract provide flexibility for the evolution of applicable technological standards? Include requirements that the vendor maintain legacy systems until your company has transitioned to a new system and that the vendor continue to provide updates for old systems.
- Set forth the parties’ respective responsibilities in the event of any regulatory changes in applicable U.S. or foreign law -- parties should commit to working together to remove impediments to fulfilling the contract, continue performing the services. Your company should have the right to terminate the

agreement if the vendor or the arrangement is not in compliance with all applicable law, or if your company's U.S. regulators object to the arrangement.

- Fluctuations in currency may need to be taken into account in the pricing and payment terms.
- The vendor should be prohibited from changing its service facilities without your company's prior written consent.
- The vendor should be prohibited from changing its operating system/interfaces without your company's prior written consent.
- The contract should specify the number and level of experience of vendor's dedicated middle managers on the ground in the foreign facility and responsible for regulatory compliance, the meeting of service standards, and other oversight and monitoring responsibilities.

- It may be necessary for the contract to specify the level and extent of employee qualifications and vendor training of the employees.
- In the event of a service interruption or other problem, the contract should provide for an escalation tree up to management of both parties.
- With respect to insurance coverage, your company may want to require business interruption/continuity coverage, war and terrorism coverage.
- The vendor should represent and warrant that it will comply with all applicable U.S. and foreign laws (including equal employment opportunity and anti-discrimination laws) and that it will indemnify your company from any losses related to its non-compliance.

- Vendor must agree to adequately maintain all records relating to the offshoring arrangement, cooperate in providing a second set of documentation in English for your company's domestic office, and agree that it will comply with and submit to examination, supervision and information requests from your U.S. regulators, including submission to and cooperation with on-site examinations.
- The contract should include carve-outs from any limitations of liability for breach of confidentiality and gross negligence or willful misconduct.
- If the services involve on-line service and web-linking to third-party websites, additional customer disclosures and protections may need to be addressed.

## **VII. Additional Compliance Concerns.**

Offshoring presents some additional compliance concerns:

- **Identity Theft Concerns.** The contract should include as necessary (such as in a business processing contract) additional protections against identity theft and strong incident reporting language, with requirements that both the vendor and your company have in place a tailored written response program for a security breach included in their respective information security plans.
- **Specific Privacy Laws.** Depending on the type of business being outsourced, attention may need to be paid to special privacy concerns, such as website on-line privacy compliance (On-line Privacy Protection Act, “OPPA”), medical privacy

(Health Insurance Portability and Accountability Act, “HIPAA”), protection for children’s privacy (Children’s On-line Privacy Protection Act, “COPPA”), and protection for school or other specific records (various state and federal laws). Compliance issues may also arise if the services involve web-linking to third party sites. Compliance with applicable telemarketing laws may also be required.

- **Anti-Money Laundering (USA PATRIOT Act/Bank Secrecy Act) Requirements.** In addition to these concerns, a vendor’s information security and business continuity plan may need to include anti-terrorism measures/considerations. Business processing and certain other agreements may require that the vendor commit to comply with your company’s anti-money laundering (“AML”) policies and

procedures. The vendor may need to develop its own AML compliance program.

- **Export Control Laws.** Compliance with federal regulations enacted pursuant to the Export Administration Act of 1979 as amended (50 U.S.C. App. 2401 *et seq.*, continued pursuant to Executive Order 13222, August 17, 2001) are often overlooked in outsourcing arrangements. Under the federal Export Administration Regulations (“EAR”) and other export control regulations, your company may be barred from exporting certain technology to the vendor, even though the vendor may be utilizing the technology only to perform the services on behalf of your company. Under the EAR, products, software or technology that is sent from the U.S. to a foreign destination may be considered to be “exported” and may require a license from the Bureau of Industry and

Security (“BIS”). The license conditions include certain record-keeping requirements. “Exportation” includes not only shipping or transferring covered goods abroad, but may also include carrying information into a foreign country on a laptop, or giving technology to a foreign national in the United States (a non-U.S. citizen or green card holder, usually in the U.S. on an H or L visa), even if that person is an employee of your company (the “deemed export rules”). “Technology” under these regulations is broadly defined to include technology processing. The restrictions on exporting various types of “dual use” technology, such as encryption technology and certain telecommunications equipment, are particularly stringent. Violation of the EARs can result in civil and criminal penalties.

- **OFAC compliance.** Both your company and the vendor may need to comply with Office of Foreign Assets Control (“OFAC”) regulations. This would include checking the names of individuals, companies and countries against the federal government’s Specially Designated Nationals (“SDN”)/Blocked Persons or entities, and sanctioned countries lists. It also includes, however, conducting ongoing due diligence to ensure that vendors your company is dealing with are not affiliated with blocked companies in sanctioned countries, *e.g.*, an Indian subsidiary or other affiliate of an Iranian company; or that your company or the vendor are not in any way facilitating transactions with SDNs/Blocked Persons or entities or with sanctioned countries.
- **Anti-boycott regulations.** Attention needs to be paid as well to compliance by your company and the vendor with the anti-

boycott regulations of the Internal Revenue Service and the Department of Commerce (BIS), which require that your company and/or its vendors do not in any way assist or facilitate unsanctioned foreign boycotts against U.S. allies. Both your company and its vendors may need to have policies and procedures, including training and reporting procedures, adopted for complying with the anti-boycott regulations. The vendor and its employees must be able to identify and reject any language in their contracts with suppliers, customer and business partners which might commit the vendor to support unauthorized boycotts. (Language in effect boycotting transactions with Israel is the usual example.)

- **Foreign Corrupt Practices Act.** Both your company and its vendors may have to comply with the federal Foreign

Corrupt Practices Act (“FCPA”), as well as with any applicable foreign anti-bribery laws, in their dealings with suppliers, customers, business partners, and others. Although the FCPA specifically prohibits businesses from bribing a foreign government official in order to obtain business or to secure an improper business advantage, compliance with the FCPA also entails avoiding doing business with foreign government officials who are known or suspected to be corrupt. Again, diligence about the vendor and who the vendor is doing business with is important.

## **VIII. Tax Issues.**

The business incentives for many offshoring arrangements are based on currently available U.S. tax deductions for offshore

business expenses and on tax and business incentives under the applicable foreign jurisdiction.

- Because the availability of U.S. deductions and foreign business incentives may change at any point during the term of the offshoring contract, provisions need to be added to the contract to allow flexibility in the pricing structures and termination rights in the event that the tax and business incentives materially change.
- The parties' respective responsibilities to pay taxes should be clearly set forth in the agreement. For example, if your company agrees to pay sales, use, and excise taxes and tariffs, it should require a resale or exemption certificate from the vendor for taxes that are invoiced to the vendor and reimbursed by your company.

## **IX. Local Law Issues/Enforceability.**

A good understanding of the applicable foreign laws that may affect the offshoring arrangement is important. As discussed above, an assessment needs to be made of the specific local law risks with respect to the particular business being outsourced. A review of the contract by foreign counsel before signing will usually be necessary.

- In the privacy area, it is important to understand how the foreign jurisdiction's data protection law meshes with the U.S. privacy law requirements, as well as those of the European Union's and those of other foreign jurisdictions where your company has customer relationships. The contract should

include vendor management dedicated to data protection oversight and compliance.

- If the outsourcing arrangement involves intellectual property rights, careful assessment of the foreign jurisdiction's intellectual property law regime is required. For example, some regimes may require specific documentation for copyright assignments. Piracy of intellectual property rights is common, even widespread, in the foreign countries most known for outsourcing activities. Even where adequate “work for hire” or similar provisions are found in the local law and captured in the contract, the law “on the books” may not reflect the local enforcement reality. In some foreign jurisdictions, law enforcement may lack the resources or the competency to pursue intellectual property thefts and the

criminal system may be slow and otherwise encumbered. (India is often cited as an example of this. It is also often cited as an example of a jurisdiction in which courts are unlikely to award large damages for breach of contract.)

- Good diligence on the law enforcement/criminal justice system in the foreign jurisdiction is important for all aspects of protecting your company's interests against the wrongful acts of employees and other parties. For example, is there an effective way to conduct background checks in the foreign jurisdiction, irrespective of what is committed to in the contract? For example, in some countries, there is no central depository of fingerprint and/or criminals records, making effective employee background checks impossible.

- Knowledge of local labor laws and how they will impact the vendor's operations are also key areas of concern.
- Review of local law issues needs to take into account any applicable treaties or conventions that exist between the U.S. and the foreign jurisdiction, or that exist between the U.S. and other nations which impact the services being rendered.